U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

REMARKS

As an initial matter, the applicants thank the examiner for his reconsideration of the case. By way of this response, claims 1, 5-9, 12, 17-20, 33, 37-42, 44, 48-51, and 54-69 remain pending and at issue, with claims 1, 12, 33, 44, 54, 59, and 63 being independent. As explained below, it is respectfully submitted that all pending claims are in condition for allowance and favorable reconsideration is respectfully requested.

Claims 1, 5-9, 12, 17-20, 33, 37-42, 44, 48-51, 54-57, 59-63, and 69:

Turning to the art rejections, the Office action rejects claims 1, 5-9, 12, 17-20, 33, 37-42, 44, 48-51, 54-57, 59-63, and 69 as unpatentable over Tsukamoto et al. (U.S. Pat. No. 5,796,828), in view of Yim (U.S. Pat. No. 6,810,387). The applicants respectfully traverse each of the rejections.

The applicants respectfully submit that independent claims 1, 12, 33, 44, 54, and 59 are patentable over the applied combination of Tsukamoto et al. and Yim. Each of the independent claims recites a method, an apparatus, or a computer-readable medium that alters a bit pattern of data bits by inverting bits in selected bit positions of the data bits and/or scrambling bits in the selected bit positions of the data bits within a hardware platform. None of the cited references, whether taken alone or in combination, teaches or suggests such a method, an apparatus, or a computer readable medium.

While Tsukamoto et al. generally discloses a satellite television broadcasting system that stores and retrieves data signals, there is no teaching or suggestion of altering a bit pattern of data bits by inverting bits in selected bit positions of the data bits and/or scrambling bits in the selected bit positions of the data bits within a hardware platform. Instead, the system of Tsukamoto et al. includes an access controller that enables/disables an encipherer prior to storing a video program on a storage medium. The access controller selectively enables and disables the encipherer based on access-control signals transmitted by a broadcasting station.

Page 12 of 18

U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

For example, the access controller disables the encipherer in response to a "full-access" signal so that a video program can be unconditionally recorded (i.e., unencrypted) on a storage medium and reproduced. See Tsukamoto et al., col. 5, lines 10-16 and col. 6, lines 32-46. In another example, the access controller enables the encipherer in response to a "no repro" signal so that the video program is encrypted prior to recording the video program on the storage medium. See Tsukamoto et al., col. 6, lines 47-59. The focus of Tsukamoto et al. is to control the encryption operation (e.g., via the encipherer) of the receiving system based on a command from the broadcasting station (e.g., a central or head end location controls the manner in which a video program is recorded onto a medium). In fact, it was acknowledged on page 3 of the Office action dated April 5, 2004, and again on page 3 of the Office action dated November 18, 2004, that Tsukamoto et al. fails to disclose or suggest altering a bit pattern of data bits by inverting bits in selected bit positions of the data bits and/or scrambling bits in the selected bit positions of the data bits.

To cure the deficiencies of Tsukamoto et al., the examiner attempts to use Yim. Yim is directed to a copy prevention apparatus and method in a digital broadcasting receiving systems that protects information stored in a storage medium from being illegally duplicated. In particular, Yim discloses a storage system including a scrambler used to scramble a video signal using an decrypted key, a key encryption unit to encrypt the key before storage, and a hard drive interface to store both the scrambled data together with the encrypted scrambler key on a storage device. See Yim, Abstract and col. 3, line 65 to col. 4, line 38. col. 16, lines 17-25.

Contrary to the assertions in the Office action regarding the Yim disclosure, Yim requires the extraction and decryption of a key from a broadcasted data signal, the descrambling of a video signal utilizing the decrypted key, the rescrambling of the video signal utilizing the key, the encryption of the key, and the storing of both the rescrambled video signal

Page 13 of 18

U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

and the encrypted key. In other words, Yim discloses the scrambling of bits according to a separately broadcasted encryption key. See Yim, col. 4, lines 9-14. In sharp contrast, the claims recite the scrambling of bits in selected bit positions. It is respectfully submitted that this is different than scrambling in response to broadcasted keys. Therefore, Yim simply does not teach or suggest the limitations of the present claims, and therefore, cannot be relied upon to overcome the deficiencies of Tsukamoto.

Accordingly, because none of the cited references teaches or suggests altering a bit pattern of data bits by inverting bits in selected bit positions of the data bits and/or scrambling bits in the selected bit positions of the data bits within a hardware platform, it follows that no combination of these references can render independent claims 1, 12, 33, 44, 54, and 59 obvious.

Furthermore, there is no motivation to combine the system disclosed in Tsukamoto et al. with Yim, because there is no motivation to modify the already protected data storage of Tsukamoto et al. with a more complicated data storage teaching of Yim.

Specifically, as stated, Tsukamoto et al. generally discloses a satellite television broadcasting system that stores and retrieves encrypted data signals. Tsukamoto et al. includes an access controller that enables/disables an enchipher (22) that encrypts, according to an encryption key, descrambled video signals supplied by descrambler (21A) to produce encrypted video signals for recording. See Tsukamoto et al., col. 4, lines 4-10. In fact, as noted by Tsukamoto et al., "the encrypted video signals cannot be displayed by ordinary means." See Tsukamoto et al., col. 4, lines 11-12, emphasis added.

As described above, Yim is directed to a copy prevention apparatus and method in a digital broadcasting receiving systems that protects information stored in a storage medium from being illegally duplicated. In particular, Yim discloses a system including a scrambler, a key encryption unit, and a hard drive interface used to store both scrambled data together with

Page 14 of 18

U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

an encrypted key. See Yim, Abstract and col. 3, line 65 to col. 4, line 38. col. 16, lines 17-25.

In other words, Yim requires the separate extraction and decryption of a key from an encrypted, scrambled data pattern, the descrambling of a data signal utilizing the key, the rescrambling of the data signal utilizing the key, the encryption of the key, and the storing of both the rescrambled data signal and the encrypted key.

While both Tsukamoto and Yim are directed toward the protection of stored data, there no motivation to combine the system disclosed in Tsukamoto et al. with Yim. Specifically, Tsukamoto et al. is focused on selectively encrypting and decrypting a video program based on an access-control signal to prevent the display of stored data by ordinary means, while Yim is focused on rescrambling a video program based on a key, encrypting the key to prevent unauthorized access to the key, and storing both the rescrambled signal and the encrypted key. In other words, Tsukamoto et al. already prevents the unauthorized display of data bits by encrypting the data stream and storing the encrypted data, (See Tsukamoto col. 4, lines 10-12), while Yim prevents the unauthorized copying of the stored data by requiring both the scrambling of the video program and the encrypting of a key.

Despite the Office action's suggestion that one of ordinary skill in the art would have been motivated to combine the rescrambling and encryption of Yim with the encryption of Tsukamoto et al. "to prevent unauthorized use of data bits," there is no motivation to combine the two references, as to replace the Tsukamoto et al. system, which selectively encrypts and decrypts data signals, with the rescrambling and key encryption processing system of Yim would destroy the Tsukamoto et al. system by requiring the Tsukamoto et al. system to broadcast an encrypted key, decrypt the key at the receiver, and provide a receiver with the additional functionality of a scrambler/descrambler unit to rescramble the video signal in conjunction with the broadcasted key. Because it is known to one of ordinary skill in the art to provide a system in which broadcast bandwidth requirements are reduced, and to provide

Page 15 of 18

U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

receivers with as few processing components as possible, there is no motivation to modify the already protected data storage of Tsukamoto et al. with the more complicated data storage teachings of Yim.

Still further, as noted in the present application, the introduction of public/private encryption keys (e.g., separately broadcasted encryption keys) introduces a number of undesirable results. For example, while some drive manufacturers "offer data encryption as the data is written to the disk and decryption as it is retrieved," (e.g., Tsukamoto) and that security "could be enhanced with public/private key encryption," (e.g., Yim), it is also noted that such an approach is undesirable as it both "complicates warranty repairs and other field support issues," as well as "introduces latency in the recording and replaying of the content." See page 3 of the application.

Accordingly, there is no motivation to combine the system disclosed in Tsukamoto et al. with Yim, because any combination of Tsukamoto et al. and Yim, not only would (1) destroy the Tsukamoto et al. system by requiring the Tsukamoto et al. system to broadcast an encrypted key, decrypt the key at the receiver, and provide a receiver with the additional functionality of a scrambler/descrambler unit to rescramble the video signal in conjunction with the broadcasted key, but (2) the proposed system would introduce inherent deficiencies associated with encryption key technology. Therefore, each of the Independent claims and all claims depending therefrom are allowable over the cited art.

Claims 5 and 37:

In regard to dependent claims 5 and 37, None of the cited references nor their combination, even if there were motivation for such a combination, discloses or suggests wherein the altering and the restoring are performed by a hard disk drive interface. Specifically, Tsukamoto discloses that the encryption and decryption are performed separately by the encipherer (22) and the decipherer (25), respectivelely, and not by the

Page 16 of 18

U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

recording/reproducing section (23A), as asserted by the Office action. In particular, Tsukamoto et al. clearly states that "encipherer 22 encrypts, according to an encryption key, descrambled video signals ... to produce encrypted video signals," and that the "encrypted video signals are supplied to recording/reproducing section 23A for recording." See col. 4, lines 4-12.

Similarly, Yim discloses that the scrambling and encrypting portion of the data processing are separately handled by the scrambler (200) and the key encryption unit (202), respectively, and not by the hard disk drive interface unit (110). See col. 3, line 65 – col. 4, line 5. Accordingly, none of the cited references nor their combination, even if there were motivation for such a combination, teaches or suggests the claimed subject matter. Therefore, each of the dependent claims 5 and 37 is allowable over the cited art.
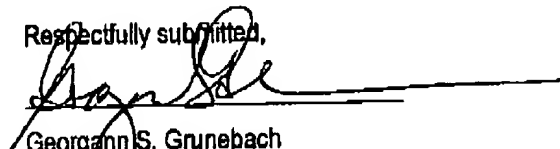
U.S. Serial No. 09/729,010
Response to the Office Action of November 18, 2004

Conclusion

For at least these reasons, it is respectfully submitted that the pending claims are in condition for allowance. If, for any reason, the examiner is unable to allow the application in the next Office action, the examiner is encouraged to telephone the undersigned attorney at the telephone number listed below.

The Commissioner is hereby authorized to charge any deficiency in the amount enclosed or any additional fees which may be required during the pendency of this application under 37 CFR 1.16 or 1.17 to Deposit Account No. 50-0383.

Respectfully submitted,

Georgann S. Grunebach
Registration No. 33,179
Attorney for Applicant

Dated: February 15, 2005

The DIRECTV Group, Inc.
RE / R11 / A109
P.O. Box 956
2250 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: (310) 964-4615